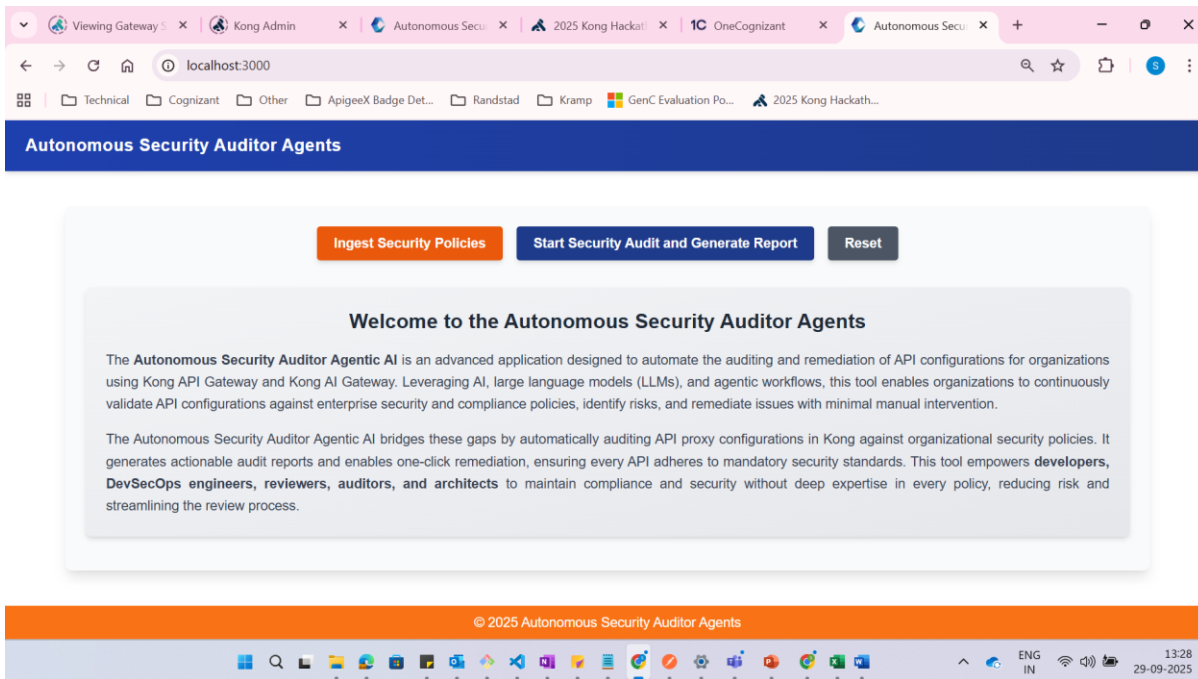
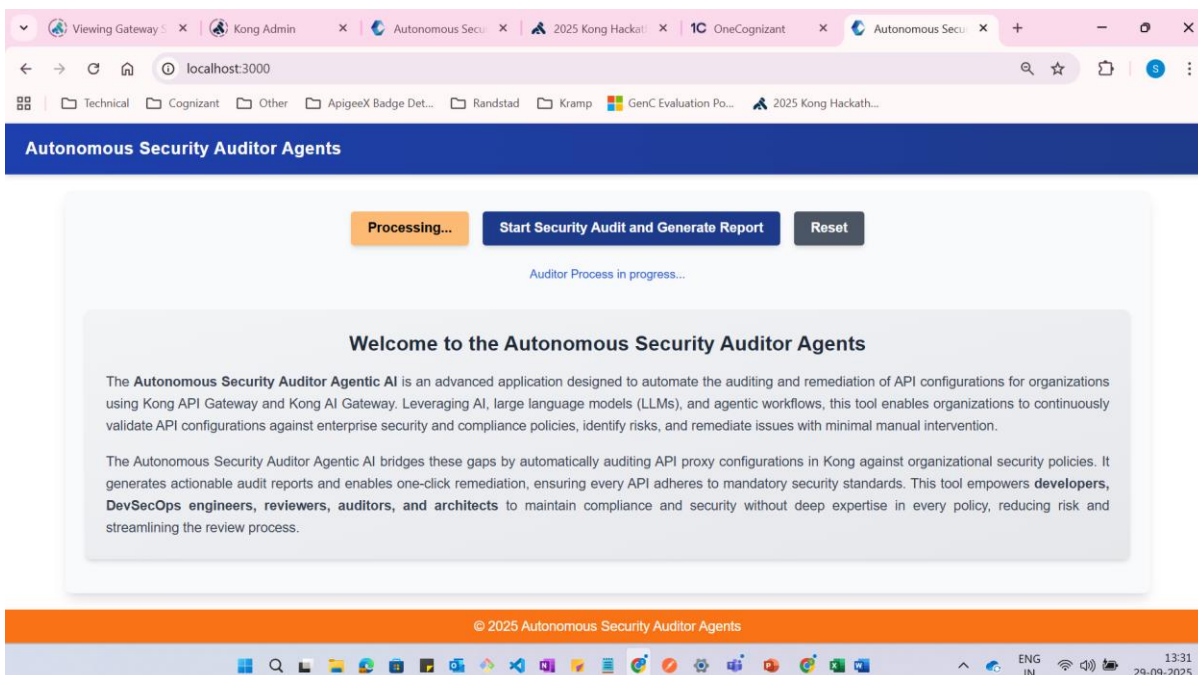


User Manual – Steps of Execution for Autonomous Security Auditor Agents

1. Home Page (After Login)



2. Ingest Organization Security Policies



Viewing Gateway x Kong Admin x Autonomous Secu x 2025 Kong Hackat x 1C OneCognizant x Autonomous Secu x

localhost:3000

Technical Cognizant Other ApigeeX Badge Det... Randstad Kramp GenC Evaluation Po... 2025 Kong Hackath...

Autonomous Security Auditor Agents

All Security Policies Ingested successfully!

Ingest Security Policies

Start Security Audit and Generate Report

Reset

Security Policies Ingested Report

Index Name	Chunk ID	Content	Metadata
security_auditor_index	ab85fcef-716e-4e49-9560-4f4df64143dd	<div>Policy Name: Authentication Policy v1.0 Description: This policy outlines the authentication mechanisms supported by Kong Gateway to ensure secure access to APIs and services. It includes mandatory and optional plugins that can be configured to enforce authentication. Mandatory Plugins to Comply to</div>	<div>{'filename': '01_authentication_policy.txt', 'chunk_id': 'ab85fcef-716e-4e49-9560-4f4df64143dd', 'timestamp': 1759132940.1763124, 'source': 'api_policies'}</div>
security_auditor_index	ba2c0ecc-42af-45f8-8eaa-19bb0ac11ef4	<div>this policy: jwt, oauth2, key-auth</div>	<div>{'filename': '01_authentication_policy.txt', 'chunk_id': 'ba2c0ecc-42af-45f8-8eaa-19bb0ac11ef4', 'timestamp': 1759132940.7533195, 'source': 'api_policies'}</div>
		<div>Policy Name: Authorization Policy v1.0 Mandatory Plugins to Comply to this policy: acl</div>	<div>{'filename': '03_authorization_policy.txt',</div>

13:32 29-09-2025

3. Audit Kong API Configurations (Audit AI Agent)

Viewing Gateway x Kong Admin x Autonomous Secu x 2025 Kong Hackat x 1C OneCognizant x Autonomous Secu x

localhost:3000

Technical Cognizant Other ApigeeX Badge Det... Randstad Kramp GenC Evaluation Po... 2025 Kong Hackath...

Autonomous Security Auditor Agents

Ingest Security Policies

Running Audit...

Reset

Auditor Process in progress...

Welcome to the Autonomous Security Auditor Agents

The **Autonomous Security Auditor Agentic AI** is an advanced application designed to automate the auditing and remediation of API configurations for organizations using Kong API Gateway and Kong AI Gateway. Leveraging AI, large language models (LLMs), and agentic workflows, this tool enables organizations to continuously validate API configurations against enterprise security and compliance policies, identify risks, and remediate issues with minimal manual intervention.

The Autonomous Security Auditor Agentic AI bridges these gaps by automatically auditing API proxy configurations in Kong against organizational security policies. It generates actionable audit reports and enables one-click remediation, ensuring every API adheres to mandatory security standards. This tool empowers **developers, DevSecOps engineers, reviewers, auditors, and architects** to maintain compliance and security without deep expertise in every policy, reducing risk and streamlining the review process.

© 2025 Autonomous Security Auditor Agents

13:33 29-09-2025

Viewing Gateway Kong Admin Autonomous Secu 2025 Kong Hackat 1C OneCognizant Autonomous Secu

localhost:3000

Technical Cognizant Other ApigeeX Badge Det... Randstad Kramp GenC Evaluation Po... 2025 Kong Hackath...

Autonomous Security Auditor Agents

Audit Completed successfully!

Ingest Security Policies

Start Security Audit and Generate Report

Reset

Security Audit Report

Sr. No.	Service Name	Security Policy Name	Compliance Status	Missing Plugins	Details
1	ApigeeToKongGenAIService	Traffic Encryption Policy	Non-Compliant	"acl" "ip-restriction"	The service is missing 'acl' or 'ip-restriction' plugins required to restrict access to trusted clients under the Traffic Encryption Policy.
2	ApigeeToKongGenAIService	Rate Limiting Policy	Non-Compliant	"rate-limiting"	The service does not have 'rate-limiting' plugin enabled, which is required to protect against abuse under the Rate Limiting Policy.
3	ApigeeToKongGenAIService	Logging Policy	Non-Compliant	"http-log" "file-log" "syslog" "loggly" "tcp-log" "udp-log"	At least one logging plugin (e.g., 'http-log', 'file-log') is required for the Logging Policy, but none are enabled on this service.

13:34

29-09-2025

Viewing Gateway Kong Admin Autonomous Secu 2025 Kong Hackat 1C OneCognizant Autonomous Secu

localhost:3000

Technical Cognizant Other ApigeeX Badge Det... Randstad Kramp GenC Evaluation Po... 2025 Kong Hackath...

Autonomous Security Auditor Agents

Audit Completed successfully!

Download Audit Report

Run Remediation Plan

Security Audit Report

4	HealthService	Traffic Filtering Policy	Non-Compliant	"ip-restriction" "acl"	The ip-restriction and acl plugins are mandatory to restrict and filter access as required by the Traffic Filtering Policy.
5	ApigeeToKongGenAIService	Authentication Policy	Compliant	-	-
6	HealthService	Authentication Policy	Compliant	-	-
7	HealthService	Request Transformation Policy	Compliant	-	-
8	KongTest	Authentication	Compliant	-	All required authentication plugins (one or more of basic-auth, key-auth, oauth2) are present.
9	KongTest	Rate Limiting	Compliant	-	rate-limiting plugin is enabled as required by this policy.
10	KongTest	IP Restriction	Compliant	-	ip-restriction plugin is enabled as required by this policy.

© 2025 Autonomous Security Auditor Agents

13:34

29-09-2025

4. Remediate Audit Report and Generate Remediation Plan (Remediate Agent)

The screenshot shows the Kong Admin interface with an audit report for the 'udp-log' policy. The report lists 10 items, with item 4 being non-compliant. Below the table are buttons for 'Download Audit Report' and 'Generating Remediation Plan...'. The status 'Loading remediation plan...' is also visible.

ID	Service Name	Policy Name	Compliance Status	Issue	Details
4	HealthService	Traffic Filtering Policy	Non-Compliant	"ip-restriction" "acl"	The ip-restriction and acl plugins are mandatory to restrict and filter access as required by the Traffic Filtering Policy.
5	ApigeeToKongGenAIService	Authentication Policy	Compliant	-	-
6	HealthService	Authentication Policy	Compliant	-	-
7	HealthService	Request Transformation Policy	Compliant	-	-
8	KongTest	Authentication	Compliant	-	All required authentication plugins (one or more of basic-auth, key-auth, oauth2) are present.
9	KongTest	Rate Limiting	Compliant	-	rate-limiting plugin is enabled as required by this policy.
10	KongTest	IP Restriction	Compliant	-	ip-restriction plugin is enabled as required by this policy.

Buttons: Download Audit Report, Generating Remediation Plan... (Loading remediation plan...)

The screenshot shows the Kong Admin interface with a remediation plan. It lists two items that need remediation: 'ApigeeToKongGenAIService' with 'Traffic Encryption Policy' and 'ApigeeToKongGenAIService' with 'Rate Limiting Policy'. The plan includes details on missing plugins and recommended actions.

Service Name	Policy Name	Issue	Missing Plugin(s)	Recommended Action	Severity
ApigeeToKongGenAIService	Traffic Encryption Policy	Missing mandatory access control and network restriction plugins.	acl, ip-restriction	Enable the 'acl' and/or 'ip-restriction' plugins to restrict API access to trusted clients only.	Medium
ApigeeToKongGenAIService	Rate Limiting Policy	Rate limiting controls are not in place to prevent API abuse.	rate-limiting	Enable and configure the 'rate-limiting' plugin to protect against API abuse and denial-of-service attacks.	Medium

Buttons: Download Audit Report, Run Remediation Plan

Viewing Gateway x Kong Admin x Autonomous Secu x 2025 Kong Hackath x 1C OneCognizant x Autonomous Secu x

localhost:3000

Technical Cognizant Other ApigeeX Badge Det... Randstad Kramp GenC Evaluation Po... 2025 Kong Hackath...

Download Audit Report Run Remediation Plan

in	Severity	Owner	Estimated Effort	Impact	Security Standard Reference
	Medium	API Security Team	2 hours	Without proper access control, unauthorized clients may access sensitive API endpoints, increasing the risk of data exposure or misuse.	OWASP API Security Top 10:2019 - API4:2019 Lack of Resources & Rate Limiting, NIST SP 800-53 AC-3, ISO 27001 A.9.1.2
	Medium	API Security Team	1 hour	Lack of rate limiting may lead to service degradation or outages due to abuse or automated attacks.	OWASP API Security Top 10:2019 - API4:2019 Lack of Resources & Rate Limiting, NIST SP 800-53 SC-5
	Medium	API Security Team	2 hours	Insufficient logging hinders detection of suspicious activities and	OWASP API Security Top 10:2019 - API10:2019 Insufficient Logging & Monitoring, GDPR Article 30, ISO 27001 A.12.4.1

13:37 29-09-2025